The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RICHARD PAUL TARQUINI

Appeal No. 2006-2430
Application No. 10/003,747

ON BRIEF

Before BARRY, BLANKENSHIP, and MACDONALD, Administrative Patent Judges.

BLANKENSHIP, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 from the examiner's final rejection of claims 1-19, which are all the claims in the application.

We affirm-in-part.

BACKGROUND

The invention relates to intrusion detection or prevention systems on computer networks that are intended to avoid attacks on targeted networks or devices.

Representative claims 1 and 17 are reproduced below.

1. A method of preventing intrusions on a node of a network, comprising;

monitoring, by a first layer of an intrusion prevention system, application data of applications running at on [sic] the node;

monitoring, by a second layer of the intrusion prevention system, transport layer data of the node; and

monitoring, by a third layer of the intrusion prevention system, network layer data of the node.

17. A node of a network, comprising:

a central processing unit;

a memory module for storing data in machine readable format for retrieval and execution by the central processing unit; and

an operating system comprising a network stack comprising a protocol driver, a media access control driver, the memory module storing an instance of an intrusion protection system application operable to monitor application layer data and an intrusion prevention system transport service provider layer, and the operating system having an intrusion prevention system network filter service provider bound to the media access control driver and the protocol driver.

The examiner relies on the following references:

Vaidya	US 6,279,113 B1	Aug. 21, 2001 (filed Jun. 4, 1998)
Holland III, et al. (Holland)	US 6,851,061 B1	Feb. 1, 2005 (filed Aug. 24, 2000)

We refer to the Final Rejection (mailed Aug. 3, 2005) and the Examiner's Answer (mailed Jun. 9, 2006) for a statement of the examiner's position and to the Brief and the Reply Brief (both filed Mar. 16, 2006) for appellant's position with respect to the claims which stand rejected.

Claims 1, 5-9, and 14-16 stand rejected under 35 U.S.C. § 102 as being anticipated by Vaidya.[1]

Claims 2-4, 10-13, and 17-19 stand rejected under 35 U.S.C. § 103 as being unpatentable over Vaidya and Holland.

OPINION

The examiner finds instant claim 1 to be anticipated (35 U.S.C. § 102) by Vaidya. As stated at column 4, lines 28 through 30, the Vaidya system monitors all seven layers of the OSI model, which necessarily includes the three application, transport, and network data layers of the seven.

Appellant argues (e.g., Brief at 7-8) that the column 4 section of Vaidya does not disclose or suggest monitoring of the three layers as set forth in claim 1. According to appellant, Vaidya extracts header information from a data packet, which is not the same as monitoring layer data by different layers of an intrusion detection system as claimed.

[1] Claim 14 is not listed in the examiner's rejection, but depending claim 16 is. Appellant's briefs acknowledge that claim 14 is included in the § 102 rejection over Vaidya.

Vaidya teaches that the prior art with respect to Vaidya's invention did not enable detecting network intrusions lower than the application layer of the OSI model. Col. 1, l. 63 - col. 2, l. 13. Vaidya's contribution to the art includes a virtual processor 36 (Fig. 4) for monitoring network data 46 to determine whether the data is associated with a network intrusion. A register cache 40 temporarily stores information extracted from a data packet. The virtual processor 36 obtains a data packet from a queue and extracts MAC header information, IP header information, transport header information, and application information from the data packet. Extraction of the packet information enables the data collector 10 to detect network intrusions based in the different layers of the OSI model. Col. 7, ll. 11-23.

Figure 5 of Vaidya demonstrates extraction of the MAC, IP, and transport header information, in addition to the application information. The different types of packet information enable generation of attack signature profiles that can recognize network intrusions based in the different layers of the OSI model. Col. 8, ll. 40-56. Moreover, communications protocols may be monitored at the network, transport, or application layers for particular attack signatures. Col. 10, ll. 22-44.

Upon review of the entirety of the reference, we consider Vaidya to provide ample support for the examiner's finding of anticipation. Nothing in appellant's briefs persuades us otherwise. We sustain the rejection of claim 1 and of claims 5-9 and 14-16, not separately argued by appellant.

We turn to the rejection of claims 2-4, 10-13, and 17-19 under 35 U.S.C. § 103 as being unpatentable over Vaidya and Holland. For dependent claims 2-4 and 10-13, appellant relies on the arguments presented in response to the rejection of base claims 1 and 9. (Brief at 8.) Since appellant's arguments do not demonstrate error in the rejection of the dependent claims, we sustain the rejection of claims 2-4 and 10-13.

However, for the reasons expressed by appellant at pages 8 and 9 of the Brief, we do not sustain the rejection of claim 17, nor of depending claims 18 and 19. The statement of the rejection of claim 17 does not address all the limitations of claim 17 but seems to address limitations from some other claim. Moreover, claim 17 relates to an intrusion prevention system (Fig. 6) as applied to a specific network stack (Fig. 3) that is not described in the applied prior art. We do not find disclosure or suggestion in Vaidya or Holland for at least an intrusion prevention system transport service provider layer as required by the claim. Further, as appellant indicates, the "filter" relied upon by the rejection is a packet filter 37 (Holland Fig. 2) in a prior art system that, according to Holland's teachings, contains significant drawbacks (e.g., col. 5, l. 8 et seq.).

CONCLUSION

The rejection of claims 1, 5-9, and 14-16 under 35 U.S.C. § 102 as being anticipated by Vaidya is affirmed.

The rejection of claims 2-4, 10-13, and 17-19 under 35 U.S.C. § 103 as being unpatentable over Vaidya and Holland is affirmed with respect to claims 2-4 and 10-13 but reversed with respect to claims 17-19.

The examiner's decision is thus affirmed-in-part.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 CFR § 1.136(a). See 37 CFR § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

LANCE LEONARD BARRY
Administrative Patent Judge)
)
)
)
)
HOWARD B. BLANKENSHIP) BOARD OF PATENT
Administrative Patent Judge) APPEALS
) AND
) INTERFERENCES
)
)
)
ALLEN R. MACDONALD)
Administrative Patent Judge)

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400